Outrage without consequences? Post-Snowden discourses and governmental practice in Germany

Dimmroth, Katharina; Steiger, Stefan; Schünemann, Wolf J.

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 7–16
DOI: 10.17645/mac.v5i1.814

Article

Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany

Stefan Steiger [1,*], Wolf J. Schünemann [2] and Katharina Dimmroth [3]

[1] Institute of Political Science, Heidelberg University, 69115 Heidelberg, Germany;
E-Mail: stefan.steiger@ipw.uni-heidelberg.de
[2] Institute of Social Sciences, Hildesheim University, 31141 Hildesheim, Germany;
E-Mail: wolf.schuenemann@uni-hildesheim.de
[3] Institute of Political Science, Rheinisch-Westfälische Technische Hochschule Aachen, 52074 Aachen, Germany;
E-Mail: katharina.dimmroth@ipw.rwth-aachen.de

* Corresponding author

Submitted: 31 October 2016 | Accepted: 20 January 2017 | Published: 22 March 2017

Abstract
In 2013 Edward Snowden's disclosures of mass surveillance performed by US intelligence agencies seriously irritated politicians and citizens around the globe. This holds particularly true for privacy-sensitive communities in Germany. However, while the public was outraged, intelligence and security cooperation between the United States and Germany has been marked by continuity instead of disruption. The rather insubstantial debate over a so-called "No-Spy-Agreement" between the United States and Germany is just one telling example of the disconnect between public discourse and governmental action, as is the recent intelligence service regulation. This article considers why and where the "Snowden effect" has been lost on different discursive levels. We analyze and compare parliamentary and governmental discourses in the two years after the Snowden revelations by using the Sociology of Knowledge Approach to Discourse (SKAD) to dissect the group-specific statements and interpretive schemes in 287 official documents by the German Bundestag, selected ministries and agencies within the policy subsystem. These will be analyzed in reference to actual governmental practice.

Keywords
cyber security; discourse analysis; dispositive analysis; German–US intelligence cooperation; surveillance

Issue
This article is part of the issue "Post-Snowden Internet Policy", edited by Julia Pohle (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

1. Introduction

When the Snowden revelations exposed the extensive surveillance practices established by the US National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) in June 2013, international criticism loomed large. Among US allies, Germany has been one of the most vocal critics of the revealed surveillance measures. Chancellor Angela Merkel most prominently expressed German discomfort in October 2013, when she said "spying among friends is completely unacceptable" (Troianovski, Gorman, & Torry, 2013). While criticism was also expressed in parliament and a commission of inquiry was set up in early 2014, actual cooperation with the US remained relatively stable. Furthermore, in 2016 the federal government proposed a new legislative framework for the German foreign intelligence agency Bundesnachrichtendienst (BND) that was approved by the German Bundestag in October of the same year. The new law, according to many experts (Bäcker, 2016; Papier, 2016; Wetzling, 2016), legalizes extensive governmental surveillance practices and may even be unconstitutional.

It is this seemingly paradoxical mismatch between harsh criticism and stable cooperation that we are going to analyze within the scope of this article. Our main research questions are therefore: How is it possible that Germany was a vocal critic of the revealed spy practices and nevertheless maintained a stable cooperation with the US? As even a superficial look into the public and political debates in Germany reveals, there has clearly been a "Snowden effect" in Germany, which has brought the issue of mass surveillance to the fore of public policy. Why has it not led to a significant change in regulation or the practices of governmental agencies? Where and why did the Snowden effect get lost within different discourse formations (parliamentary, governmental)?

Up to now, research on governmental reactions to the Snowden revelations has been published only scarcely. When discussed, German government reactions have been covered with a focus on arguments legitimizing surveillance measures (Schulze, 2015). We will go further by also analyzing the parliamentary debate and investigating the practical implications of possible discursive shifts with a deeper look into the dispositives (institutions, regulations and practices). In the existing literature, one can identify slightly different perspectives on the German reaction to the disclosed practices. These views seem to be facilitated by an emphasis on either practical consequences or rhetoric. Emphasizing the harsh criticism following the revelations, Bersick, Christou and Yi (2016, pp. 176–177) state that:

> In the case of Germany, the Snowden affair even undermined the general belief in the normative foundations of the US–German relationship and gave rise to previously unheard-of criticism of the United States by German members of the federal cabinet.

Other scholars emphasized that practical relations (especially security cooperation) between the US and Germany remained stable in the aftermath of the revelations. Segal (2016, p. 150) concludes that "even at the zenith of the public backlash, cooperation between the US and German intelligence agencies never stopped". Segal tentatively argues that this reaction was motivated by the German "dependence on US intelligence capabilities" (Segal, 2016, p. 143), but his claim is not built on significant empirical data from the German administration or parliament. We would like to substantiate this debate and take those findings as a starting point for our analysis. We agree with Bersick et al. (2016) that leading politicians in Germany voiced strong criticism against the US (and the UK) regarding the revelations, and we also acknowledge in concurrence with Segal (2016) that practical implications remained marginal, as is clearly underlined by the latest developments. But together, both observations set the puzzle that we are investigating.

In order to provide an answer to our research questions, the article will proceed in four steps. The next section lays out our framework for discourse analysis and specifies our methodological approach. To illustrate the reluctant German reactions, the third section presents a short analysis of the most important practical events following the Snowden revelations; this part sheds light on the measures the German government has actually taken to deal with the revelations. Our empirical analysis of governmental and parliamentary discourse is then presented in the fourth section. A final conclusion sums up our findings.

2. Discourses, Dispositives and What Happens in between: Theory and Methodology

Discourse research has gained ground in political science in recent years (pars pro toto: Hajer, 2002; Howarth, Norval, & Stavrakakis, 2000; Wodak & Krzyzanowski, 2008). Even in international relations and security studies, discourse analysis (DA) has become more popular, and the scope of DA methodology has considerably broadened (for cyber security and online communication issues see for instance: Balzacq, 2011; Gorr & Schünemann, 2013; Xiao Wu, 2012). First of all, we adhere to a Foucauldian discourse theory (Foucault, 2002), which makes the discourse a socio-historically specific knowledge formation that appears materially manifested in social communication. Moreover, we apply an approach developed from the combination of Foucauldian discourse theory and the Sociology of Knowledge tradition in sociology. The Sociology of Knowledge Approach to Discourse ([SKAD] Keller, 2008) has been developed by German sociologist Reiner Keller since the late 1990s. One crucial advantage of SKAD in relation to other discourse analytical approaches is that it brings the actor back into focus. SKAD furthermore provides the analyst with a research framework encompassing a set of basic interpretive schemes, which complement the interpretive analytics otherwise adopted from Foucault.

Corpus-building is one of the first and most important steps of any solid discourse research. For this study, we chose an actor-oriented approach. This was relatively easy for the parliamentary debate, as we selected all Bundestag protocols dealing with cyber security issues by using the search function of the official Bundestag database, entering the search terms "cyber security" and "cyber attack". We cut and parsed the resulting protocols to include only the sections that dealt with the relevant issue, since a single Bundestag debate may deal with a variety of topics. For governmental actors and agencies, we identified ministries and investigative authorities as the key actors in German cyber security policy, i.e. the policy subsystem (Sabatier, 1988). The identified actors were the Federal Government, the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defense, the Federal Ministry for Economic Affairs and Energy, the Federal Ministry of Justice and Consumer Protection and the Federal Office for Information Security. We continued our document-gathering by entering the same query terms of "cyber security"

("Cybersicherheit") and "cyber attack" ("Cyberangriff") using the search functions provided by the ministries' websites. The query terms had been intuitively selected and then validated using the "relative query term relevance" (RQTR) method proposed by Costas Gabrielatos (2007). The period of analysis spans the two years following the Snowden revelations, i.e. June 1, 2013, to May 31, 2015. The governmental documents we identified by using our query terms ranged from official ministry reports, interviews and speeches to press releases. Our final corpus for analysis consisted of 287 documents in total, 156 of which came from government offices and 131 from parliament.

As to our interpretive analysis, we analyze our corpus first for the recurrent statements and then look, in accordance with SKAD methodology, for all sorts of interpretive schemes (some call them frames) included therein. These patterns of interpretation can again be divided into subtypes such as narratives, classifications or subject positions (Keller, 2008). While statements are thus the basic analytical unit for a discourse analysis, being based on the social actors' worldview, i.e. how people make sense of the world around them, the interpretive scheme is the overarching analytical category towards which the more concrete and specific interpretive codes of the researcher are oriented. Our case, for example, raises the question of whether the newly disclosed surveillance activities amount to illegal espionage and a breach of trust, or whether they are seen and justified as a legitimate part of a protective role and, thus, an example of successful intelligence cooperation.

In addition to SKAD, the Foucauldian term of the dispositive is also of particular importance for this study. The dispositive—in the Foucauldian sense and as adopted by Keller—is an umbrella term for all sorts of power-effects through which a discourse leaves its lasting mark on the world and/or the organization of a given society. While the discourse is a practice itself and it appears as materialized practice as well, it is still necessarily transient as knowledge elements are being processed all the time and never reach a fixed state. However, they do have long lasting effects on the world and the ordered living of a society through established practices, regulations, and institutions. The dispositive thus includes "material objects (buildings, technologies, etc.), practices (such as the execution of punishments) and elements in the form of texts (such as the adoption of laws)" (Keller, 2013, pp. 78–79). Changes in regulatory discourses on public security will likely lead to institutionalization and intervention into the material world or into the rulebook of a society. The same can be expected of data protection or cyber security issues. The "privacy by design" guideline, for instance, which has become almost common sense in many regulatory discourses, is increasingly being institutionalized in laws or guidelines that could be labeled as a data protection dispositive. The sequential and causal logic is not as clear-cut as the examples so far suggest. Of course, dispositives have repercussions for discourses as well. The concept of the dispositive encompasses not only the effects discourses have on the world but also the very infrastructure of discourse production: "The concept of dispositive means the bundle of measures that carries a discourse and transposes it into real-world consequences" (Keller, 2007, p. 50, translation by the authors). This also makes sense and can be illustrated with reference to the cyber security subsystem. The dispositive includes privileged speaker positions (such as the ministers of the interior or the chancellery) as well as fora of discourse production (such as the "NSA-Untersuchungsausschuss" or the Parliamentary Control Committee).

3. German Reactions to the Snowden Revelations

In one of her first public reactions to the revelations in July 2013, Chancellor Merkel already expressed her concerns by highlighting that not all technical possibilities should actually be used to facilitate surveillance, but she also expressed sympathy for different needs for security in the US and Germany (Federal Government, 2013). In this statement, she also announced a program to enhance privacy in order to deal with the new situation. One of the program's key elements took shape in cooperation with the Brazilian government. Both Chancellor Merkel and then President Dilma Rousseff were among the most prominent surveillance targets and were therefore very critical of the practices revealed by Snowden. Together both governments drafted a UN-resolution to ensure privacy in the digital age. Resolution 68/167 was passed by the United Nations General Assembly after some debate in December 2013 (UN, 2013). The resolution emphasized:

> that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society. (UN, 2013, p. 2)

The passing of the resolution also closely coincided with a new embarrassment for the German government when surveillance of Angela Merkel's cell phone was disclosed in October (Smale, 2013). While this reaction is connected to privacy concerns frequently articulated in public and parliamentary discourses, it is remarkable that the intergovernmental UN General Assembly was selected as a regulatory forum. Given the non-binding character of UN resolutions, it does not imply any change in practice, not even by the German government as one of the initiators of the resolution.

In contrast, the establishment of a commission of inquiry (the "NSA-Untersuchungsausschuss") by the German Bundestag in January 2014 can be seen as a concrete step to re-evaluate the established intelligence cooperation. Its task is not only to further investigate accu-

sations against the US and British intelligence agencies but to also clarify the activities of German agencies. Another concrete measure, which even entailed a change of practices, came when the federal government, after negotiations on a "no-spy-agreement" had failed, changed its practice of contracting a foreign provider by recalling contracts with Verizon in June 2014. Until then the government had tasked the US-based enterprise with providing services for its telecommunications infrastructure. Consequently, Verizon was replaced by Deutsche Telekom (Hudson, 2014). The decision to replace a US-based company by a German competitor can be seen as clearly rooted in the pursuit of digital sovereignty (see DA below).

In contrast, the temporal and partial disruptions of the German–US intelligence cooperation that started in May 2015 (Connolly, 2015), while being an obvious change in the practices of information sharing, were more of symbolic value. Information sharing was halted when it became public that the NSA had used its cooperation with the German BND to spy on targets within Germany and the European Union (EU). But the change only affected the cooperation in Bad Aibling and, following an investigation, cooperation was re-established in January 2016 (Mascolo, 2016).

Finally, in June 2016 the German government presented a new legal framework for the foreign surveillance activities of the BND (Federal Chancellery, 2016). Since the draft enabled easier information sharing between intelligence agencies and weakened previously established limitations on data collection (Papier, 2016), it was met with considerable criticism. NGOs and journalists argued that the government had legalized previously illegal activities and thereby enhanced the surveillance capabilities of the German intelligence agency (Deutscher Journalisten-Verband, 2016; Meister, 2016). Furthermore, critique was also expressed by representatives of the Organization for Security and Co-operation in Europe (OSCE) and the UN (OSCE, 2016; UN, 2016). Nevertheless, the government remained committed to the new legislative framework and parliament finally passed the new law in October 2016.

As this short summary clearly shows, the German government responded quite reluctantly to the revelations and resorted to more symbolic reactions. In 2016 the government even began to enhance surveillance capabilities. These developments were enabled by different governmental and parliamentary discourses that will be analyzed in the following section.

4. Post-Snowden Discourses Compared: The Debates in the German Bundestag and the Governmental Discourse

In the course of our discourse analysis in the wake of the Snowden revelations, we identified five recurrent discursive elements that seem particularly important for understanding what happened to the Snowden effect in German policy-making. Therefore, we compare how the respective discursive elements differ between the statements of parliamentary and governmental speakers. What is modified and in what way? What gets lost? What is added? How does all this influence the (un)likelihood of a change in practices?

4.1. Reduced Need to Act—The Parliamentary Discourse

4.1.1. The Fundamental Problem—The Tense Relation between Freedom and Security

One of the prevalent discursive trends in parliament after the Snowden revelations strikes at the very heart of the matter, explicitly addressing the tension between freedom and security, which most speakers agree needs to be re-balanced either towards security (with regard to terrorism and potential attacks) or towards freedom. Determining the measures necessary to balance the security and physical wellbeing of the citizens with their right to freedom and privacy is of course the key issue for politicians of all affiliations in the context of the NSA affair.

Most parliamentary speakers tend to come down on the side of freedom:

> These rights to freedom must be protected—against an overly powerful surveillance state, for example—because the quest for complete security leads to tyranny and a lack of freedom. To quote an American, Benjamin Franklin: Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety. Manfred Grund, CDU/CSU (Deutscher Bundestag, 2014)

This speaker stands out in particular as his statements provide one of the few explanations for the emphasis on one societal good over another:

> Freedom is a very important good. It is in fact the most important good of our constitution. There's a reason the enumeration of civil liberties is at the very beginning of our constitution. Manfred Grund, CDU/CSU (Deutscher Bundestag, 2014)

This is one of the clearest examples of a parliamentarian explaining the prioritization of freedom over security. The Grundgesetz serves as a point of reference, since the rights ensuring freedom for the average German citizen are the first to be documented in the constitution. Additionally, a notable moment in parliamentary discourse is brought about when one of the members references the "super fundamental right of security", a term coined by Interior Minister Friedrich, to make the opposing argument:

> In our negotiations and discussions we'll now make it very clear that there is a super fundamental right

> to freedom in the United States as well as here at home, and we'll make it clear that the Federal Government [of Germany] isn't perceiving this affair as being concluded by a long shot. Michael Hartmann, SPD (Deutscher Bundestag, 2014)

The call for freedom isn't particularly surprising given the massive privacy invasions the Snowden revelations brought to light. Nonetheless, while the importance of freedom is invoked, in many cases its absolute value is diluted by mentioning its close relationship with security concerns. The very existence of the freedom v. security framing points to the fact that none of the speakers are disregarding the importance of security as a societal good. This implies a preparedness for concessions and may indicate parliamentary tolerance for non-action on the part of the government.

4.1.2. Digital Sovereignty—The Struggle for Digital Autonomy

With digital sovereignty, we coded one remarkable interpretive scheme through which the current distribution of power in cyberspace and the German dependence on other forces (above all the US) is vehemently challenged. The respective demand is made quite often in parliamentary debate. It is almost always rooted in the context of the EU regulatory framework, in which higher autonomy seems achievable. Hence, speakers mostly call to develop a European digital strategy:

> Ladies and Gentlemen, in light of the excessive data-gathering by the NSA, it is our central task in Germany and Europe to reclaim sovereignty over what is done with our data. We need legal and technical means to do that. Günter Krings, CDU/CSU (Deutscher Bundestag, 2014)

The argument for a renewed sovereignty in the digital realm also points to the problem of the asymmetrical dependence on the US. This dependence is stated explicitly in the following example:

> This is not about IT-nationalism, but if we take an honest look at the situation, we have to admit that we're dependent on US or Asian software and hardware in many instances. We need our own initiatives in the areas of research and development. Lars Klingbeil, SPD (Deutscher Bundestag, 2014)

It is acknowledged that other state actors such as the US and Asian countries possess more resources in the area of digital development, something Germany isn't able to compete with, at least at the moment. Developing the ability to counter these dependencies is given high importance in the wake of the Snowden revelations. The text sequences coded with the digital sovereignty scheme are the ones that most clearly challenge the current relations and practices between Germany and the US regarding security issues and intelligence.

4.1.3. Cyber Angst—The New Level of Threat in the Digital Age

A frequently appearing narrative in both discourses underscores the elevated need for security in reaction to a higher threat level in the digital age affecting both states and citizens. This narrative, which we coded with the term "cyber angst", explores the many potential threats cyberspace poses to a state's security. This includes possible terrorist attacks on critical infrastructure as well as criminal activity in the cyber realm. The narrative serves a securitization logic (Buzan, Waever, & de Wilde, 1998), as it is prone to justifying extraordinary surveillance measures. So-called cyber angst, particularly regarding critical infrastructure, is a crucial narrative in the governmental discourse. It is also found in the parliamentary debate:

> We need online security, especially within the area that's important for our society and country. Communication on a state level must be safe. If we want to uphold critical infrastructure it has to be safe from hacking, attacks and espionage. Hans-Peter Uhl, CDU/CSU (Deutscher Bundestag, 2013a)

4.1.4. Post Privacy—It's a New World

There is another narrative that might serve to reduce the severity and thus lessen the impact of the Snowden revelations within the parliamentary debate. Like cyber angst, it is also rooted in the newness and paradigm-shifts that are ascribed to internet development and the digital era. Cyberspace is depicted by some advocates as such a new and foreign world that some normative prescriptions, as central as they may be, cannot fully apply. This narrative implies that modern societies have moved towards a post-privacy age. Following that argument, the actions of the US government are not justified per se, but the societal norm of privacy that is in danger is depicted as already compromised:

> We shouldn't let citizens believe that they're still safe from espionage if they disclose private matters online. We have to make that clear, especially to young people using Facebook and Twitter among other things. We have to tell them that everything they put online stays there and that there's no digital eraser. That's an illusion. We have to tell people that. Hans-Peter Uhl, CDU/CSU (Deutscher Bundestag, 2013a)

The post-privacy narrative comes with another important implication: the blame for a privacy breach is put not only on firms or state agencies that conduct surveillance, but is also attributed to online users who freely share private information on the internet. The responsibility

shifts to citizens, as they are expected to know that information shared online at any time might be the target of corporate or government espionage. Given the overwhelming regulatory demands that internet communication confronts us with, the best line of defense is seen in self-regulation instead of government intervention.

4.1.5. Asymmetrical Dependence in the Security Realm

An effective interpretive scheme that potentially reduces any activism supporting a path-breaking turn in security cooperation with the US is the continued reminder that Germany is highly dependent on US intelligence in security matters. This asymmetrical dependence is brought up many times:

> Every single one of us knows that attacks in Germany were prevented by US intelligence, that's part of the truth of this debate. But we also have to think about how we'll prevent future surveillance. Michael Grosse-Brömer, CDU/CSU (Deutscher Bundestag, 2013b)

This statement addresses a need to prevent surveillance in Germany, while at the same time stating the absolute necessity of US–German cooperation in the security realm to prevent terrorist attacks. This discursive element is the most overt in explaining Germany's continued intelligence and security cooperation with the United States in spite of the Snowden revelations. The bottom line of this logic seems to be that while Germany condemns the surveillance, there simply is no other option to safeguard domestic security apart from cooperating with the US. Additionally, there is an element of gratefulness towards the US for its role in preventing attacks in Germany, which may inhibit harsh criticism of their surveillance activities. One speaker addresses the impossibility of truly faulting the US for its actions while at the same time relying on them for intelligence:

> It won't impress the Americans if we rightly and legitimately criticize their actions in the NSA affair, but at the same time, in Germany and Europe, allow our own defense efforts to erode to the point that we always have to ask for data and insights from the US agencies when things get serious. Günter Krings, CDU (Deutscher Bundestag, 2013b)

If we follow this argument, German officials are in no position to criticize the US for its surveillance activities as they provide the very same intelligence that has kept German citizens safe in the past. The speaker states that even the legitimate criticism will more than likely fall on deaf ears in the US if its allies in Europe take few measures to ensure their own safety and are thus reliant on their partner overseas. The implied solution is the development of intelligence capabilities by Germany and other European states to lessen the dependence on US intelligence and gain some equality in the security relationship and open a dialogue on these matters.

4.2. Refused Need to Act—The Governmental Discourse

4.2.1. The Fundamental Problem—The Tense Relation between Freedom and Security

Explicit reflections on the relationship between security and freedom are even more frequent in the governmental discourse. There are distinct differences to the way parliamentarians discussed it. Representatives in the Bundestag mainly prioritize freedom over security, while government officials talk about security as a transcendental good, i.e. a good without which other goals, including freedom, cannot be achieved:

> Security is the prerequisite for freedom. Hans-Dieter Heumann (Federal Academy for Security Policy, 2015)

When even freedom is seen and depicted as dependent on security, it is not far to the statement of then Minister of the Interior Hans-Peter Friedrich emphasizing security as a "super fundamental law" (Bewarder & Jungholt, 2013). If there can be no freedom without security, the mass surveillance by the US government could even be portrayed as a way of ensuring freedom instead of endangering it. While this is not uttered explicitly, the implications help to understand why meaningful change in cooperative practices with the US is not only regarded as not feasible, but also as not necessary in the end. Furthermore, one governmental document addresses the varying response to the freedom v. security struggle in different countries and puts this down to different historical experiences:

> The balance of freedom and security takes various shapes in different states for historical reasons. (Ministry of the Interior, 2013)

Even though it is only implied here, the idea is that the US surveillance is rooted in historical experiences that make them more likely to come down on the side of security, particularly the terrorist attacks of 9/11. This is a sympathetic view that seeks to somewhat justify US intelligence activities, as they have been employed after a traumatic event that would cause a state to be hypervigilant in security matters.

4.2.2. Digital Sovereignty—The Struggle for Digital Autonomy

Standing in contrast to the other recurrent elements, demands for digital autonomy or sovereignty are articulated in a clearer fashion within the governmental discourse than in the parliamentary debate. The idea that Germany must achieve a sort of digital sovereignty—

mostly in cooperation with the EU—to break free of US influence was supported even by the German Minister for the Interior de Maizière:

> Our political leverage is significantly defined by our technological capabilities. Therefore, we have to do everything possible to maintain IT capabilities in order to keep and further build our own technological platforms….The government is going to develop a strategy to secure national competitiveness. I've already said that this is a modern form of patriotism. Thomas de Maizière (Ministry of the Interior, 2014a)

In this speech, de Maizière also emphasized that the EU is crucial to achieving this goal. This also shows that even though the need for independence from US cooperation is acknowledged, Germany is not seen as being capable of achieving this goal alone, i.e. outside of the cooperative framework of the EU. The idea of building a European counterbalance to US hegemony in digital matters is one of the few ways in which the Snowden revelations seem to have had a disruptive effect on US–German cooperation.

4.2.3. Cyber Angst—The New Level of Threat in the Digital Age

The narrative that cyberspace is exposing states and their citizens to a higher level of risk is much more frequently used in the governmental discourse than in parliament. There are also differences in the way how it is told. Moreover, the implied claims are presented with much more certainty as are the derived solutions:

> A stable, secure, open and free internet offers great opportunities: for economic growth and development, for good governance and democracy, as well as for social exchange between people around the world. At the same time, it confronts us with new threats: Numerous states are pursuing military cyber-capabilities, which might lead to an atmosphere of mutual distrust and conflict. Private actors have shown great skill in abusing the net for criminal purposes. Terrorists have been using the internet for their means. Norbert Riedel (Ministry of Foreign Affairs, 2015a)

This quote offers insight into the way this particular narrative unfolds. While some positive effects of the cyber age are acknowledged, the dangers posed by this new way of dealing with the world are exposed at the same time. In this instance, two different kinds of threats are addressed: the atmosphere of distrust created by this new way states can attack each other and the possibility of terrorists and criminals using the internet for their own purposes. In its entirety, this narrative creates an atmosphere of fear and implicitly justifies using extraordinary means—e.g. mass surveillance—to ensure the security of a state or society. This comes down to a securitization logic with government officials as the prime securitizing agents (Buzan et al., 1998).

4.2.4. Post Privacy—It's a New World

While the cyber angst narrative is more important for the governmental discourse than for the parliamentary one, the opposite is true of the narrative according to which cyberspace has brought about a kind of post privacy era, as it is much less prominently represented in governmental discourse than it is in the parliamentary debate. Nevertheless, the narrative is employed as well:

> In a changing world that requires answers for the continued digitalization of our society and newly developing areas of organization, we cannot simply fall back on our ordinary patterns of behavior and keep rigid systems that don't live up to the challenges of this day and age. Norbert Riedel (Ministry of Foreign Affairs, 2015b)

In this instance, the narrative of cyberspace as a new frontier is used to challenge the outdated strategies used to deal with these new circumstances. From this perspective, a more extreme argument would be possible by which the revealed mass surveillance of the NSA is seen as a coping technique employed to deal with the new challenges cyberspace poses to states and their governments.

4.2.5. Asymmetrical Dependence in the Security Realm

In contrast to the previous example, there is not much difference in how the idea of an asymmetrical security relationship between Germany and the US appears in governmental and parliamentary discourses. Rather, this seems to be more or less common sense:

> The United States is our most important partner and our closest ally. The security cooperation with our US partners is irreplaceable in regards to our domestic and external security. That's especially true for the fight against terrorism. This is the reason we want to continue and deepen our cooperation. Thomas de Maizière (Ministry of the Interior, 2014b)

The demand in this quote from Minister of the Interior de Maizière is very clear: given the high dependence of German security on US intelligence information, there is no other option to guarantee the security of Germany than to continue the close security cooperation with the US. He even goes further by expressing a desire to deepen the already existing cooperation instead of reducing it. The way de Maizière frames the cooperation doesn't imply that it is a necessary evil brought about by Germany's own lack of intelligence capabilities in certain areas. On the contrary, he explicitly names the US as the closest partner and ally, a role that German government officials

apparently take no objection to even in the wake of the Snowden revelations. Considering how the actions of the US government have widely been interpreted as a betrayal of its allies, this hints at a relationship that runs very deeply indeed.

5. Conclusion

Considering the outrage the Snowden revelations provoked in German public discourse, one could have expected that politicians would react to it with a bundle of measures to reform policies, institutions and practices in the security realm. From this perspective, it seemed likely that especially the close security cooperation with the US would be restrained by more privacy-sensitive regulation in this field. However, as we all know by now, the consequences of the Snowden revelations for the German–US intelligence collaboration have been few and far between. Security cooperation with the US remained stable most of the time, and the government even extended the capabilities of German intelligence agencies with a new legal framework for foreign surveillance. The reforms that have been carried out are rather symbolic in nature, but some even legalize the revealed practices instead of trying to forbid them. This discrepancy between public statements and government action is the puzzle that our research started with. We approached the problem with a discourse analytical framework. Relying on the Sociology of Knowledge Approach to Discourse, we comparatively analyzed parliamentary and governmental discourses in Germany after the Snowden revelations.

In our empirical sections, we identified five recurrent elements that could be found in parliamentary and governmental discourses that facilitated the reluctant reactions in different ways. The first one included all general and/or explicit reflections on the tense fundamental relationship between freedom and security and is thus rather indifferent regarding the expected consequences; the debate seems to favor neither side overwhelmingly and an absolute call for security is rarely made. Additionally, we found a push for digital sovereignty or autonomy which clearly effected a change of practice with the German government canceling its contract with Verizon. While this element certainly influenced the move away from a contractor based in the US, the dependencies addressed also include concerns about Asian companies, therefore leading to more nuanced thoughts about which dependencies might be less problematic and how to avoid them altogether.

While the two elements mentioned above can potentially either increase or decrease cooperation with the US, we also found three recurrent elements which all serve to reduce the perceived severity of the NSA scandal and thus prevent more resolute efforts to reduce cooperation with the US. The first one we called cyber angst. This element expresses a diffuse anxiety about the new threats in our increasingly digital world. Fears are stoked about state and non-state actors using cyberspace to forward their (malicious) goals at the expense of German society, leading to calls for a more active state response and more cooperation among trusted allies. The second element consists of post-privacy narratives. These focus on the distinct newness of cyberspace and argue that standards established in the offline world might not be suitable for the digital world; far reaching surveillance measures may eventually be normal conduct in the new medium. Furthermore, the state might not be the most dangerous actor in this field after all, since big companies are also engaged in extensive data collection. A reluctant response was further facilitated by the argument of asymmetrical dependence. This element emphasizes the German dependence on the US in the realm of security policy. Proponents of this argument stress the fact that cooperation with US intelligence agencies helps to protect German citizens. This is often combined with a reference to the important role the US has played in German history. It is argued that even if surveillance might be problematic, the US is not the most dangerous threat to Germany, since there are far more problematic actors that need to be countered. This argument thereby also seamlessly connects to the cyber angst narratives.

All in all, given the initial public outrage, the alleged Snowden effect seems to have diminished over time through an apparent cascade in sequential logic in the public discussions examined here. We could identify a considerable difference between the discourses in parliament and government. The need for change or stronger regulation seems reduced already by what is said and argued in the parliamentary debates. Any call for a considerable regulation that might cause a disruption in German–US security cooperation is almost completely disregarded in the governmental discourse.

Acknowledgements

We acknowledge financial support by Deutsche Forschungsgemeinschaft and Ruprecht-Karls-Universität Heidelberg within the funding programme Open Access Publishing.

Conflict of Interests

The authors declare no conflict of interests.

References

Bäcker, M. (2016). Stellungnahme zu dem Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes. *Deutscher Bundestag*. Retrieved from http://www.bundestag.de/blob/459630/1ddfe2451c0fd067872976d0f0467882/18-4-653-g-data.pdf

Balzacq, T. (2011). A theory of securitization. Origins, core assumptions, and variants. In T. Balzacq (Ed.), *Securitization theory. How security problems emerge and dissolve* (pp. 1–30). London: Routledge.

Bersick, S., Christou, G., & Yi, S. (2016). Cybersecurity and EU–China relations. In. E. J. Kirchner, T. Christiansen, & H. Dorussen (Eds.), *Security relations between China and the European Union* (pp. 167–186). Cambridge: Cambridge University Press.

Bewarder, M., & Jungholt, T. (2013, July 16). Friedrich erklärt Sicherheit zum "Supergrundrecht". *Welt*. Retrieved from https://www.welt.de/politik/deutschland/article118110002/Friedrich-erklaert-Sicherheit-zum-Supergrundrecht.html

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Rienner.

Connolly, K. (2015, May 7). German secret service BND reduces cooperation with NSA. *The Guardian*. Retrieved from https://www.theguardian.com/world/2015/may/07/german-secret-service-bnd-restricts-cooperation-nsa-us-online-surveillance-spy

Deutscher Bundestag. (2013a). Stenografischer Bericht 249. Sitzung Berlin, Mittwoch, den 26. Juni 2013. *Deutscher Bundestag*. Retrieved from http://dip21.bundestag.de/dip21/btp/17/17249.pdf

Deutscher Bundestag. (2013b). Stenografischer Bericht 2. Sitzung Berlin, Montag, den 18. November 2013. *Deutscher Bundestag*. Retrieved from http://dip21.bundestag.de/dip21/btp/18/18002.pdf

Deutscher Bundestag. (2014). Stenografischer Bericht 7. Sitzung Berlin, Mittwoch, den 15. Januar 2014. *Deutscher Bundestag*. Retrieved from http://dip21.bundestag.de/dip21/btp/18/18007.pdf

Deutscher Journalisten-Verband. (2016, September 16). BND-Gesetz. Kein Schutz für Journalisten. *Deutscher Journalisten-Verband*. Retrieved from http://www.djv.de/startseite/profil/der-djv/pressebereich-download/pressemitteilungen/detail/article/kein-schutz-fuer-journalisten.html?cHash=cad80f8c0f4108ced1be30a704676f24&type=500

Federal Academy for Security Policy. (2015). Cyber-Realität zwischen Freiheit und Sicherheit. *Federal Academy for Security Policy*. Retrieved from https://www.baks.bund.de/en/node/513

Federal Chancellery. (2016). Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes. *Bundeskanzleramt*. Retrieved from https://www.bundesregierung.de/Content/DE/_Anlagen/2016/06/2016-06-28-entwurf-bnd-gesetz.pdf?__blob=publicationFile&v=1

Federal Government. (2013). Deutschland ist ein Land der Freiheit. *Bundesregierung*. Retrieved from https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html;jsessionid=FA5B3F77DAD45E2755C7E47F46DED066.s7t2?nn=437032#Start

Foucault, M. (2002). *Archaeology of knowledge*. London and New York, NY: Routledge.

Gabrielatos, C. (2007). Selecting query terms to build a specialized corpus from a restricted-access database. *ICAME Journal*, *31*, 5–43.

Gorr, D., & Schünemann, W. J. (2013). Creating a secure cyberspace: Securitization in Internet governance discourses and dispositives in Germany and Russia. *International Review of Information Ethics*, *20*(12), 37–51.

Hajer, M. A. (2002). Discourse analysis and the study of policy making. *European Political Science*, *2*(1). Retrieved from http://www.maartenhajer.nl/upload/Hajer%20EPS.pdf

Howarth, D., Norval, A. J., & Stavrakakis, Y. (Eds.). (2000). *Discourse theory and political analysis. Identities, hegemonies and social change*. Manchester: Manchester University Press.

Hudson, A. (2014, June 26). German government cancels Verizon contract in wake of U.S. spying row. *Reuters*. Retrieved from http://www.reuters.com/article/us-germany-security-verizon-idUSKBN0F11WJ20140626

Keller, R. (2007). *Diskursforschung. Eine Einführung für SozialwissenschaftlerInnen*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Keller, R. (2008). *Wissenssoziologische Diskursanalyse. Grundlegung eines Forschungsprogramms*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Keller, R. (2013). *Doing discourse research: An introduction for social scientists*. London: SAGE Publications.

Mascolo, G. (2016, January 8). BND und NSA kooperieren wieder in Bad Aibling. *Süddeutsche Zeitung*. Retrieved from http://www.sueddeutsche.de/politik/abhoerskandal-bnd-und-nsa-kooperieren-wieder-in-bad-aibling-1.2810828

Meister, A. (2016, June 30). Das neue BND-Gesetz—Alles, was der BND macht, wird einfach legalisiert und sogar noch ausgeweitet. *Netzpolitik.org*. Retrieved from https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/

Ministry of Foreign Affairs (2015a). Rede des Beauftragten für Cyber-Außenpolitik, Botschafter Dr. Norbert Riedel, bei der Tagung der Freedom Online Coalition in Ulan Bator (Mongolei). *Ministry of Foreign Affairs*. Retrieved from http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2015/150504-Riedel_Freedom_Online_Coalition_Conference.html

Ministry of Foreign Affairs (2015b). Es braucht neue Regeln fürs Internet—Deutschland und Brasilien im Einsatz für Privatsphäre und Sicherheit. *Ministry of Foreign Affairs*. Retrieved from http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Interviews/2015/150330_Cyber_Privatsphaere.html

Ministry of the Interior. (2013, August). Maßnahmen für einen besseren Schutz der Privatsphäre. Fortschrittsbericht vom 14. August 2013. *Ministry of the Interior*. Retrieved from http://www.bmwi.de/BMWi/Redaktion/PDF/ST/massnahmen-fuer-einen-besseren-schutz-derprivatsphaere,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

Ministry of the Interior. (2014a). Schutz—Sicherheit—Vertrauen Auftrag der Politik im digitalen Zeitalter. *Ministry of the Interior*. Retrieved from http://www.

protokoll-inland.de/SharedDocs/Reden/DE/2014/06/dud.html

Ministry of the Interior. (2014b). Rede von Bundesinnenminister de Maizière anlässlich des 11. Symposiums des Bundesamtes für Verfassungsschutz am 8. Mai 2014 in Berlin. *Ministry of the Interior*. Retrieved from http://www.bmi.bund.de/SharedDocs/Reden/DE/2014/05/bfv-symposium.html

Organization for Security and Co-operation in Europe. (2016). Surveillance amendments in new law in Germany pose a threat to media freedom, OSCE Representative says, asks Bundestag to reconsider bill. *Organization for Security and Co-operation in Europe*. Retrieved from http://www.osce.org/fom/252076

Papier, H.-J. (2016). Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten. *Neue Zeitschrift für Verwaltungsrecht*, *35*(15), 1–15.

Sabatier, P. A. (1988). An advocacy coalition framework of policy change and the role of policy-oriented learning therein. *Policy Sciences*, *21*(2/3), 129–168.

Schulze, M. (2015). Patterns of surveillance legitimization. The German discourse on the NSA scandal. *Surveillance & Society*, *13*(2), 197–217.

Segal, A. M. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. New York, NY: PublicAffairs.

Smale, A. (2013, October 23). Anger growing among allies on U.S. spying. *New York Times*. Retrieved from http://www.nytimes.com/2013/10/24/world/europe/united-states-disputes-reports-of-wiretapping-in-Europe.html?_r=0

Troianovski, A., Gorman, S., & Torry, H. (2013, October 24). European leaders accuse U.S. of violating trust. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052702304799404579195018887172 2

United Nations. (2013). Resolution 68/167. *United Nations*. Retrieved from. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

United Nations. (2016). *Stellungnahme*. Retrieved from https://netzpolitik.org//wp-upload/2016/09/160829_Stellungnahme_UN-Sonderbeauftragte_zur_BND-Reform.pdf

Wetzling T. (2016). Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BND) sowie weiterer Vorlagen. *Deutscher Bundestag*. http://www.bundestag.de/blob/459622/a6a22e212bb9c777028554ed1ba4bbfc/18-4-653-c-data.pdf

Wodak, R., & Krzyzanowski, M. (Eds.). (2008). *Qualitative discourse analysis in the social sciences*. Basingstoke: Palgrave Macmillan.

Xiao Wu, A. (2012). Hail the independent thinker. The emergence of public debate culture on the Chinese internet. *International Journal of Communication*, *6*, 2220–2244.

About the Authors

Stefan Steiger, MA, is a research fellow and doctoral student at the Institute of Political Science of the University of Heidelberg. His main fields of interest are cyber security, internet governance and foreign policy analysis.

Wolf J. Schünemann, Dr., is Junior Professor of Political Science at Hildesheim University. His main fields of interest are internet governance, political online communication, European integration and discourse studies.

Katharina Dimmroth, MA, is a research fellow at the Institute of Political Science of RWTH Aachen University. Her main fields of interest are US and German foreign policy, cyber security and international relations.